Claims:

1. An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the decoy device comprises:

an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device, and

the firewall device comprises:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution condition; and

a filtering condition manager for managing the filtering condition depending on whether the attack detector detects an attack based on the input IP packet forwarded to the decoy device.

2. The attack defending system according to claim 1, wherein the header information of an input IP packet includes at least one of a source IP address and a destination IP address thereof,

wherein the destination selector selects a destination of the input IP packet depending on whether the header information of the input IP packet satisfies the distribution condition.

3. The attack defending system according to claim 1, wherein the destination selector comprises a memory for storing as the distribution condition a guiding list containing a set of IP addresses unused in the internal network, wherein the destination selector selects the decoy device when a destination IP address of the input IP packet matches an unused IP address contained in the guiding list.

4. The attack defending system according to claim 1, wherein the destination selector comprises:

a packet buffer for storing input IP packets; and

a monitor for monitoring reception of a destination unreachable message after an input IP packet has been transferred from the packet buffer to the internal network,

wherein, when the monitor detects the reception of the destination unreachable message for the input IP packet, the input IP packet is transferred from the packet buffer to

the decoy device.

5. The attack defending system according to claim 1, wherein the firewall device further comprises:

a distribution condition updating section for updating the distribution condition depending on whether the attack detector detects an attack based on the input IP packet transferred to the decoy device.

6. The attack defending system according to claim 1, wherein the filtering condition manager stores the filtering condition with a limited validity period, which corresponds to the header information of the input IP packet forwarded to the decoy device, wherein, when the limited validity period has elapsed, a default filtering condition is returned to the packet filter.

7. The attack defending system according to claim 1, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

8. The attack defending system according to claim 6, wherein the filtering condition manager comprises:

a condition generator for generating a filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address information of the input IP packet; and

a filtering condition controller for dynamically updating the filtering condition according to the filtering condition generated by the condition generator.

9. The attack defending system according to claim 1, wherein the decoy device comprises:

an event memory for temporarily storing events related to at least network input/output, file input/output, and process creation/termination; and

an event manager for analyzing cause-effect relations of the events stored in the event memory to form links among the events.

10. The attack defending system according to claim 1, wherein the attack detector detects an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

11. The attack defending system according to claim 9,

wherein the attack detector detects an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

12. The attack defending system according to claim 11, wherein the attack detector searches the links to extract at least, a generation event of a process generating an event to be inspected and a network reception event by which the event to be inspected is generated, when determination is made based on the domain constraint and the type constraint.

13. The attack defending system according to claim 1, further comprising a mirroring device for copying at least a file system from a server on the internal network to the decoy device, wherein when an attack is detected by the decoy device, the mirroring device copies at least the file system from the server on the internal network to the decoy device.

14. An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the firewall device comprises:

a destination selector for selecting one of the internal network and the decoy device as a destination of the

input IP packet based on header information of the input IP packet and a distribution condition; and

a confidence manager for managing confidence levels for source IP addresses of a plurality of input IP packets,

wherein the destination selector obtains a confidence level for a source IP address of the input IP packet from the confidence manager and selects a destination of the input IP packet depending on whether the confidence level satisfies the distribution condition.

15. The attack defending system according to claim 14, wherein, when a confidence level for a source IP address is retrieved, the confidence manager updates the confidence level for the source IP address.

16. The attack defending system according to claim 15, wherein the confidence manager updates the confidence level by adding a predetermined value to the confidence level for the source IP address.

17. The attack defending system according to claim 15, wherein the confidence manager updates the confidence level by adding a variable to the confidence level for the source IP address, wherein the variable becomes smaller as a packet size of the input IP packet corresponding to the confidence level becomes larger.

18. The attack defending system according to claim 15, wherein the confidence manager updates the confidence level when the input IP packet is a packet conforming to a predetermined protocol.

19. The attack defending system according to claim 14, wherein the confidence manager comprises:

a first confidence memory for storing the confidence levels for the source IP addresses of the plurality of input IP packets and latest updated times at which the confidence levels were updated, respectively;

a second confidence memory for storing a copy of the confidence levels stored in the first confidence memory;

a first updating processor for updating a confidence level stored in the first confidence memory when the destination selector has obtained the confidence level;

a copying processor for copying the confidence levels stored in the first confidence memory to the second confidence memory at regular intervals; and

a second updating processor for searching the second confidence memory for a confidence level corresponding to a latest updated time from which a predetermined time period has elapsed, to update a found confidence level.

20. The attack defending system according to claim 19,

wherein the copying processor searches the first confidence memory for a confidence level corresponding to a latest updated time from which a predetermined time period has elapsed and deletes an entry corresponding to a found confidence level from the first confidence memory.

21. The attack defending system according to claim 19, wherein the second updating processor decrease the found confidence level by a predetermined value.

22. The attack defending system according to claim 19, wherein the second updating processor deletes the found confidence level from the second confidence memory.

23. The attack defending system according to claim 14, wherein the decoy device comprises an attack detector for detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device.

24. The attack defending system according to claim 23, wherein the confidence manager updates a confidence level of a source IP address of the input IP packet transferred to the decoy device depending on whether the attack detector detects an attack based on the input IP packet transferred from the firewall device.

25. The attack defending system according to claim 14, wherein the decoy device comprises:

an event memory for temporarily storing events related to at least network input/output, file input/output, and process creation/termination; and

an event manager for analyzing cause-effect relations of the events stored in the event memory to form links among the events.

26. The attack defending system according to claim 14, wherein the decoy device comprises:

an attack detector for detecting an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

27. The attack defending system according to claim 25, wherein the decoy device further comprises:

an attack detector for detecting an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

28. The attack defending system according to claim 27, wherein the attack detector searches the links to extract at

least, a generation event of a process generating an event to be inspected and a network reception event by which the event to be inspected is generated, when determination is made based on the domain constraint and the type constraint.

29. The attack defending system according to claim 14, further comprising a mirroring device for copying at least a file system from a server on the internal network to the decoy device, wherein when an attack is detected by the decoy device, the mirroring device copies at least the file system from the server on the internal network to the decoy device.

30. An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the firewall device comprises:

a first destination selector;

a second destination selector; and

a confidence manager for managing confidence levels for source IP addresses of a plurality of input IP packets,

wherein

the first destination selector selects one of the second destination selector and the decoy device as a destination of the input IP packet based on header information of the input

IP packet and a first predetermined condition; and

the second destination selector obtains a confidence level for a source IP address of the input IP packet from the confidence manager and selects a destination of the input IP packet depending on whether the confidence level satisfies a second predetermined condition.

31. The attack defending system according to claim 30, wherein the decoy device comprises:

an event memory for temporarily storing events related to at least network input/output, file input/output, and process creation/termination; and

an event manager for analyzing cause-effect relations of the events stored in the event memory to form links among the events.

32. The attack defending system according to claim 30, wherein the decoy device comprises:

an attack detector for detecting an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

33. The attack defending system according to claim 31, wherein the decoy device further comprises:

an attack detector for detecting an attack from an

execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

34. The attack defending system according to claim 33, wherein the attack detector searches the links to extract at least, a generation event of a process generating an event to be inspected and a network reception event by which the event to be inspected is generated, when determination is made based on the domain constraint and the type constraint.

35. The attack defending system according to claim 30, wherein the decoy device and the firewall device are accommodated in a single unit.

36. The attack defending system according to claim 30, further comprising a mirroring device for copying at least a file system from a server on the internal network to the decoy device, wherein when an attack is detected by the decoy device, the mirroring device copies at least the file system from the server on the internal network to the decoy device.

37. An attack defending method using a decoy device in a firewall device provided at an interface between an internal network and an external network, comprising:

preparing a filtering condition and a distribution

condition for input IP packets;

determining whether an input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

selecting one of the internal network and the decoy device as a destination of the input IP packet accepted, based on the header information of the input IP packet and the distribution condition;

detecting presence or absence of an attack by executing a service process for the input IP packet forwarded to the decoy device; and

managing the filtering condition corresponding to the input IP packet forwarded to the decoy device depending on whether an attack is detected based on the input IP packet.

38. The attack defending method according to claim 37, wherein the header information of an input IP packet includes at least one of a source IP address and a destination IP address thereof, wherein a destination of the input IP packet is determined depending on whether the header information of the input IP packet satisfies the distribution condition.

39. The attack defending method according to claim 37, wherein the distribution condition is a guiding list containing a set of IP addresses unused in the internal network, wherein

the input IP packet is transferred to the decoy device when a destination IP address of the input IP packet matches an unused IP address contained in the guiding list.

40. The attack defending method according to claim 37, wherein the distribution condition is updated depending on whether an attack is detected based on the input IP packet transferred to the decoy device.

41. The attack defending method according to claim 37, wherein the filtering condition managing step comprises:

setting the filtering condition with a limited validity period, corresponding to the header information of the input IP packet forwarded to the decoy device; and

when the limited validity period has elapsed, setting the filtering condition to a default filtering condition.

42. The attack defending method according to claim 37, wherein the filtering condition managing step comprises:

generating a filtering condition corresponding to a combination of an attack category of an attack detected and address information of the input IP packet; and

dynamically updating the filtering condition according to the filtering condition generated.

43. The attack defending method according to claim 37, wherein the attack detecting step comprises:

temporarily storing events related to at least network input/output, file input/output, and process creation/termination; and

analyzing cause-effect relations of the events to form links among the events.

44. The attack defending method according to claim 37, wherein the attack detecting step comprises:

extracting events related to at least network input/output, file input/output, and process creation/termination; and

comparing the extracted events with a rule having domain constraint and type constraint added thereto.

45. The attack defending method according to claim 43, wherein the attack detecting step further comprises:

comparing the events with a rule having domain constraint and type constraint added thereto.

46. The attack defending method according to claim 45, wherein the links are searched to extract at least, a generation event of a process generating an event to be inspected and a network reception event by which the event to be inspected is generated, when determination is made based on the domain

constraint and the type constraint.

47. The attack defending method according to claim 44, wherein the rule describes a constraint related to an access source including a network domain and a constrain related to processes processing accesses and its sequence.

48. The attack defending method according to claim 45, wherein the rule describes a constraint related to an access source including a network domain and a constrain related to processes processing accesses and its sequence.

49. An attack defending method using a decoy device in a firewall device provided at an interface between an internal network and an external network, comprising:

preparing a distribution condition of IP packets;

holding confidence levels for source IP addresses of a plurality of input IP packets;

selecting one of the internal network and the decoy device as a destination of the input IP packet depending on whether the confidence level satisfies the distribution condition.

50. The attack defending method according to claim 49, wherein the confidence level holding step comprises:

storing the confidence levels for the source IP

addresses of the plurality of input IP packets and latest updated times at which the confidence levels were respectively updated, into a real-time confidence database;

updating a confidence level stored in the real-time confidence database each time the confidence level is accessed;

copying the confidence levels stored in the real-time confidence database to a long-term confidence database at regular intervals;

searching the long-term confidence database to find a confidence level corresponding to a latest updated time from which a predetermined time period has elapsed; and

updating a confidence level found.

51. The attack defending method according to claim 49, further comprising:

at the decoy device,

detecting presence or absence of an attack by executing a service process for the input IP packet transferred from the firewall device.

52. The attack defending method according to claim 51, further comprising:

updating a confidence level of a source IP address of the input IP packet transferred to the decoy device depending on whether an attack is detected by the decoy device based on the input IP packet transferred from the firewall device.

53. The attack defending method according to claim 51, wherein the attack detecting step comprises:

temporarily storing events related to at least network input/output, file input/output, and process creation/termination; and

analyzing cause-effect relations of the events to form links among the events.

54. The attack defending method according to claim 51, wherein the attack detecting step comprises:

extracting events related to at least network input/output, file input/output, and process creation/termination; and

comparing the extracted events with a rule having domain constraint and type constraint added thereto.

55. The attack defending method according to claim 53, wherein the attack detecting step further comprises:

comparing the events with a rule having domain constraint and type constraint added thereto.

56. The attack defending method according to claim 55, wherein the links are searched to extract at least, a generation event of a process generating an event to be inspected and a network reception event by which the event to be inspected

is generated, when determination is made based on the domain constraint and the type constraint.

57. The attack defending method according to claim 54, wherein the rule describes a constraint related to an access source including a network domain and a constrain related to processes processing accesses and its sequence.

58. The attack defending method according to claim 55, wherein the rule describes a constraint related to an access source including a network domain and a constrain related to processes processing accesses and its sequence.

59. A firewall device connected to a decoy device, provided at an interface between an internal network and an external network, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, comprising:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution

condition; and

a filtering condition manager for managing the filtering condition corresponding to the input IP packet forwarded to the decoy device depending on whether the attack detector detects an attack based on the input IP packet.

60. A firewall device connected to a decoy device, provided at an interface between an internal network and an external network, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, comprising:

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet based on header information of the input IP packet and a distribution condition; and

a confidence manager for managing confidence levels for source IP addresses of a plurality of input IP packets,

wherein the destination selector obtains a confidence level for a source IP address of the input IP packet from the confidence manager and selects a destination of the input IP packet depending on whether the confidence level satisfies the distribution condition.

61. A firewall device connected to a decoy device, provided at an interface between an internal network and an external network, wherein the firewall device inputs an input

IP packet from the external network and forwards it to one of the decoy device and the internal network, comprising:

a first destination selector;

a second destination selector; and

a confidence manager for managing confidence levels for source IP addresses of a plurality of input IP packets, wherein

the first destination selector selects one of the second destination selector and the decoy device as a destination of the input IP packet based on header information of the input IP packet and a first predetermined condition; and

the second destination selector obtains a confidence level for a source IP address of the input IP packet from the confidence manager and selects a destination of the input IP packet depending on whether the confidence level satisfies a second predetermined condition.

62. A firewall device connected to a decoy device, provided at an interface between an internal network and an external network, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, comprising:

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the packet filter, based on the header information of the input IP packet and a distribution condition;

a confidence manager for managing confidence levels for source IP addresses of a plurality of input IP packets; and

a filtering condition manager for managing the filtering condition corresponding to the input IP packet forwarded to the decoy device depending on whether the attack detector detects an attack based on the input IP packet,

wherein the destination selector obtains a confidence level for a source IP address of the input IP packet from the confidence manager and selects a destination of the input IP packet depending on whether the confidence level satisfies the distribution condition.

63. A program for implementing an attack defending system on a computer, the attack defending system including a decoy device and a firewall device, which are provided at an interface between an internal network and an external network, the program comprising:

preparing a set of filtering conditions and a distribution condition of IP packets;

determining whether an input IP packet inputted from

the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

selecting one of the internal network and the decoy device as a destination of the input IP packet accepted, based on the header information of the input IP packet and the distribution condition;

detecting presence or absence of an attack by executing a service process for the input IP packet forwarded to the decoy device; and

managing the filtering condition corresponding to the input IP packet forwarded to the decoy device depending on whether an attack is detected based on the input IP packet.

64. A program for implementing an attack defending system on a computer, the attack defending system including a decoy device and a firewall device, which are provided at an interface between an internal network and an external network, the program comprising:

preparing a distribution condition of IP packets;

holding confidence levels for source IP addresses of a plurality of input IP packets;

selecting one of the internal network and the decoy device as a destination of the input IP packet depending on whether the confidence level satisfies the distribution condition.

65. A program for implementing a firewall device on a computer, wherein the firewall is connected to a decoy device and is provided at an interface between an internal network and an external network, the program comprising:

preparing a set of filtering conditions and a distribution condition of IP packets;

determining whether an input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

selecting one of the internal network and the decoy device as a destination of the input IP packet accepted, based on the header information of the input IP packet and the distribution condition;

instructing the decoy device to detect presence or absence of an attack by executing a service process for the input IP packet forwarded to the decoy device; and

managing the filtering condition corresponding to the input IP packet forwarded to the decoy device depending on whether an attack is detected based on the input IP packet.

66. A program for implementing a firewall device on a computer, wherein the firewall is connected to a decoy device and is provided at an interface between an internal network and an external network, the program comprising:

preparing a distribution condition of IP packets;

holding confidence levels for source IP addresses of a plurality of input IP packets;

selecting one of the internal network and the decoy device as a destination of the input IP packet depending on whether the confidence level satisfies the distribution condition.

67. A decoy device in an attack defending system comprising:

an event memory for temporarily storing events related to at least network input/output, file input/output, and process creation/termination while executing a server process; and

an event manager for analyzing cause-effect relations of the events stored in the event memory to form links among the events.

68. A decoy device in an attack defending system comprising:

an attack detector for detecting an attack from an execution status of a service process according to a rule having at least one of domain constraint and type constraint added thereto.

69. The decoy device according to claim 67, further

comprising:

an attack detector for detecting an attack from an execution status of the service process according to a rule having at least one of domain constraint and type constraint added thereto.

70. The decoy device according to claim 69, wherein the attack detector searches the links to extract at least, a generation event of a process generating an event to be inspected and a network reception event by which the event to be inspected is generated, when determination is made based on the domain constraint and the type constraint.

71. An attack defending system provided at an interface between an internal network and an external network, comprising a decoy device and a firewall device, wherein the firewall device inputs an input IP packet from the external network and forwards it to one of the decoy device and the internal network, wherein

the firewall device comprises:

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet, based on request data included in the input IP packet and a distribution condition; and

a confidence manager for managing a confidence level of request data,

wherein the destination selector obtains a

confidence level of the request data included in the input IP packet from the confidence manager and determines a destination of the input IP packet depending on whether the obtained confidence level of the request data included in the input IP packet satisfies the distribution condition.

72. The attack defending system according to claim 71, wherein the destination selector selects both of the internal network and the decoy device as a destination of the input IP packet when the obtained confidence level of the request data included in the input IP packet is not smaller than a predetermined threshold.

73. The attack defending system according to claim 71, wherein the destination selector comprises an input buffer for temporarily storing the input IP packet when the obtained confidence level of the request data included in the input IP packet is smaller than a predetermined threshold,

wherein, when the decoy device verifies that the request data included in the input IP packet is safe, the destination selector automatically transfers the input IP packet from the input buffer to the internal network.

74. The attack defending system according to claim 72, wherein the destination selector comprises an input buffer for temporarily storing the input IP packet when the obtained

confidence level of the request data included in the input IP packet is smaller than the predetermined threshold,

wherein, when the decoy device verifies that the request data included in the input IP packet is safe, the destination selector automatically retransfers the input IP packet from the input buffer to the internal network.

75. The attack defending system according to claim 71, wherein the decoy device comprises:

an event memory for temporarily storing events related to at least network input/output, file input/output, and process creation/termination while executing a server process; and

an event manager for analyzing cause-effect relations of the events stored in the event memory to form links among the events.

76. The attack defending system according to claim 71, wherein the decoy device comprises:

an attack detector for detecting an attack from an execution status of a service process according to a rule having at least one of domain constraint and type constraint added thereto.

77. The attack defending system according to claim 75, wherein the decoy device further comprises:

an attack detector for detecting an attack from an execution status of a service process according to a rule having at least one of domain constraint and type constraint added thereto.

78. The attack defending system according to claim 77, wherein the attack detector searches the links to extract at least, a generation event of a process generating an event to be inspected and a network reception event by which the event to be inspected is generated, when determination is made based on the domain constraint and the type constraint.

79. The attack defending system according to claim 71, wherein the firewall device further comprises:

an encryption processor for decrypting an encrypted input IP packet and encrypting an output IP packet.

80. The attack defending system according to claim 71, further comprising a mirroring device for copying at least a file system from a server on the internal network to the decoy device, wherein when an attack is detected by the decoy device, the mirroring device copies at least the file system from the server on the internal network to the decoy device.

81. An attack detecting method in an attack defending system, comprising:

temporarily storing events related to at least network input/output, file input/output, and process creation/termination while executing a server process; and

analyzing cause-effect relations of the events stored in the event memory to form links among the events.

82. An attack detecting method in an attack defending system, comprising:

extracting events related to at least network input/output, file input/output, and process creation/termination; and

comparing the extracted events with a rule having domain constraint and type constraint added thereto.

83. The attack detecting method according to claim 81, further comprising:

comparing the events with a rule having domain constraint and type constraint added thereto.

84. The attack detecting method according to claim 83, wherein the links are searched to extract at least, a generation event of a process generating an event to be inspected and a network reception event by which the event to be inspected is generated, when determination is made based on the domain constraint and the type constraint.

85. The attack detecting method according to claim 82, wherein the rule describes a constraint related to an access source including a network domain and a constrain related to processes processing accesses and its sequence.

86. The attack detecting method according to claim 83, wherein the rule describes a constraint related to an access source including a network domain and a constrain related to processes processing accesses and its sequence.

87. An attack defending method using a decoy device in a firewall device provided at an interface between an internal network and an external network, comprising:

preparing a set of filtering conditions and a distribution condition of IP packets;

determining whether an input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

selecting one of the internal network and the decoy device as a destination of the input IP packet accepted, based on request data included in the input IP packet and the distribution condition;

detecting presence or absence of an attack by executing a service process for the input IP packet forwarded to the decoy device; and

managing the filtering condition corresponding to the input IP packet forwarded to the decoy device depending on whether an attack is detected based on the input IP packet.

88. The attack defending method according to claim 87, wherein the distribution condition is a confidence management table containing a plurality of entries, each of which comprises a combination of request data and its confidence level,

wherein the attack defending method further comprises:

when an entry matching the request data included in the input IP packet is found in the confidence management table, extracting a confidence level from the entry; and

when no entry matching the request data included in the input IP packet is found in the confidence management table, creating a new entry comprised of a combination of the request data and an initial confidence level in the confidence management table.

89. The attack defending method according to claim 88, wherein, in the destination selecting step, when the confidence level extracted from the confidence management table is not smaller than a predetermined threshold, both of the internal network and the decoy device are selected as a destination of the input IP packet.

90. The attack defending method according to claim 88, wherein, in the destination selecting step, when the confidence level extracted from the confidence management table is not smaller than a predetermined threshold, the input IP packet is temporarily stored and, if no attack is detected, then the input IP packet is automatically transferred to the internal network.

91. A program for implementing an attack detecting system on a computer, the program comprising:

temporarily storing events related to at least network input/output, file input/output, and process creation/termination while executing a server process; and

analyzing cause-effect relations of the events stored in the event memory to form links among the events.

92. A program for implementing an attack detecting system on a computer, the program comprising:

extracting events related to at least network input/output, file input/output, and process creation/termination; and

comparing the extracted events with a rule having domain constraint and type constraint added thereto.

93. A program for implementing an attack detecting system on a computer, the program comprising:

temporarily storing events related to at least network input/output, file input/output, and process creation/termination while executing a server process;

analyzing cause-effect relations of the events stored in the event memory to form links among the events; and

comparing the events with a rule having domain constraint and type constraint added thereto.

94. A program for implementing an attack detecting system on a computer, wherein the attack detecting system uses a decoy device and a firewall device provided at an interface between an internal network and an external network, the program comprising:

preparing a set of filtering conditions and a distribution condition of IP packets;

determining whether an input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and a filtering condition corresponding to the input IP packet;

selecting one of the internal network and the decoy device as a destination of the input IP packet accepted, based on request data included in the input IP packet and the distribution condition;

detecting presence or absence of an attack by executing a service process for the input IP packet forwarded to the decoy device; and

managing the filtering condition corresponding to the input IP packet forwarded to the decoy device depending on whether an attack is detected based on the input IP packet.

95. The program according to claim 94, wherein the distribution condition is a confidence management table containing a plurality of entries, each of which comprises a combination of request data and its confidence level,

wherein the attack defending method further comprises:

when an entry matching the request data included in the input IP packet is found in the confidence management table, extracting a confidence level from the entry; and

when no entry matching the request data included in the input IP packet is found in the confidence management table, creating a new entry comprised of a combination of the request data and an initial confidence level in the confidence management table.

96. The program according to claim 95, wherein, in the destination selecting step, when the confidence level extracted from the confidence management table is not smaller than a predetermined threshold, both of the internal network and the decoy device are selected as a destination of the input IP packet.

97. The program according to claim 95, wherein, in the

destination selecting step, when the confidence level extracted from the confidence management table is not smaller than a predetermined threshold, the input IP packet is temporarily stored and, if no attack is detected, then the input IP packet is automatically transferred to the internal network.

98. An attack defending system provided at an interface between an internal network and an external network, comprising:

a decoy device;

a firewall device; and

a switch device connected between the decoy device and the firewall device,

wherein

the decoy device comprises:

an attack detector for detecting presence or absence of an attack by executing a service process for an input IP packet transferred from the switch device,

the switch device comprises:

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet accepted by the firewall device, based on the header information of the input IP packet and a distribution condition; and

a condition generator for generating the filtering condition corresponding to a combination of an attack category of an attack detected by the attack detector and address

information of the input IP packet, and

the firewall device comprises:

a filtering condition controller for dynamically updating the filtering condition depending on the filtering condition generated by the condition generator; and

a packet filter for determining whether the input IP packet inputted from the external network is to be accepted, based on header information of the input IP packet and the filtering condition.

99. The attack defending system according to claim 98, wherein the switch device further comprises:

a confidence manager for managing confidence levels for source IP addresses of a plurality of input IP packets,

wherein the destination selector obtains a confidence level for a source IP address of the input IP packet from the confidence manager and selects a destination of the input IP packet depending on whether the confidence level satisfies the distribution condition.

100. The attack defending system according to claim 98, wherein the firewall device and the switch device are connected through a network.

101. An attack defending system provided at an interface between an internal network and an external network, comprising:

a decoy cluster including a plurality of decoy devices, which correspond to a server on the internal network; and

a firewall device which transfers an input IP packet to at least one selected from the server and the plurality of decoy devices,

wherein the firewall device comprises:

a confidence manager for managing a confidence level for an input IP packet; and

a server manager for managing the server by assigning at least one requisite confidence level to each of the plurality of decoy devices in the decoy cluster,

wherein, when an IP packet is inputted, the firewall device obtains a confidence level of the input IP packet from the confidence manager and determines a decoy device having a requisite confidence level, which is not greater than the obtained confidence level, as a destination of the input IP packet.

102. An attack defending system provided at an interface between an internal network and an external network, comprising:

a firewall device; and

at least one attack detecting system provided in at least one of the internal network and the external network,

wherein the firewall device comprises an alert transformation section, which receives an attack detection

alert from the at least one attack detecting system and transforms it to an alert including at least an attack-source IP address and an attack-target IP address.

103. An attack defending system provided at an interface between an internal network and an external network, comprising:

a firewall device;

a decoy device; and

at least one confidence management server,

wherein

the firewall device transmits a request message including at least a part of data of an input IP packet, to the at least one confidence management server, and

the at least one confidence management server generates a confidence level for the input IP packet from data included in the request message in response to the request message, and transmits a response message including at least the confidence level back to the firewall device.

104. The attack defending system according to claim 103, wherein the firewall device comprises:

a destination selector for selecting one of the internal network and the decoy device as a destination of the input IP packet, based on header information of the input IP packet and a distribution condition; and

a management server connection section for

transmitting the request message to the at least one confidence management server and obtaining the confidence level for the input IP packet as a response to the request message,

wherein the destination selector selects a destination of the input IP packet depending on whether the confidence level for the input IP packet satisfies the distribution condition.

105. An attack defending method in an attack defending system provided at an interface between an internal network and an external network, comprising:

preparing a plurality of decoy devices, which correspond to a server on the internal network;

holding a distribution condition used to distribute an IP packet based on at least one requisite confidence level assigned to each of the plurality of decoy devices, and confidence levels for a plurality of IP packets;

when an IP packet is inputted, obtaining a confidence level of the input IP packet; and

determining a decoy device having a requisite confidence level, which is not greater than the obtained confidence level, as a destination of the input IP packet.

106. An attack defending method in an attack defending system provided at an interface between an internal network and an external network, comprising:

preparing at least one attack detecting system provided in at least one of the internal network and the external network; and

when an attack detection alert is received from the at least one attack detecting system, transforming it to an alert including at least an attack-source IP address and an attack-target IP address.

107. A program for implementing an attack detecting system on a computer, wherein the attack detecting system is provided at an interface between an internal network and an external network, the program comprising:

assigning at least one requisite confidence level to each of a plurality of decoy devices, which correspond to a server on the internal network;

holding a distribution condition used to distribute an IP packet based on the at least one requisite confidence level and confidence levels for a plurality of IP packets;

when an IP packet is inputted, obtaining a confidence level of the input IP packet; and

determining a decoy device having a requisite confidence level, which is not greater than the obtained confidence level, as a destination of the input IP packet.

108. A program for implementing an attack detecting system on a computer, wherein the attack detecting system is

provided at an interface between an internal network and an external network, the program comprising:

receiving an attack detection alert from at least one attack detecting system provided in at least one of the internal network and the external network; and

transforming the attack detection alert to an alert including at least an attack-source IP address and an attack-target IP address.

109. An attack defending method in an attack defending system provided at an interface between an internal network and an external network, wherein the attack defending system comprises a firewall device, a decoy device, and at least one confidence management server, wherein

the firewall device transmits a request message including at least a part of data of an input IP packet, to the at least one confidence management server, and

the at least one confidence management server generates a confidence level for the input IP packet from data included in the request message in response to the request message, and transmits a response message including at least the confidence level back to the firewall device.

110. The attack defending method according to claim 109, wherein the destination selector selects a destination of the input IP packet depending on whether the confidence level for

the input IP packet satisfies the distribution condition.

111. A program for implementing an attack detecting system on a computer, wherein the attack detecting system is provided at an interface between an internal network and an external network, wherein the attack defending system comprises a firewall device, a decoy device, and at least one confidence management server, the program comprising:

receiving a request message from the firewall device, wherein the request message includes at least a part of data of an input IP packet;

generates a confidence level for the input IP packet from data included in the request message in response to the request message; and

transmitting a response message including at least the confidence level back to the firewall device.

112. A program for implementing an attack detecting system on a computer, wherein the attack detecting system is provided at an interface between an internal network and an external network, wherein the attack defending system comprises at least a decoy device, a firewall device and a confidence management server, the program comprising:

transmitting a request message from the firewall device to the confidence management server, wherein the request message includes at least a part of data of an input

IP packet;

receiving a response message from the confidence management server, the response message including at least a confidence level of the input IP packet calculated from data included in the request message; and

selecting one of the internal network and the decoy device as a destination of the input IP packet depending on whether the confidence level of the input IP packet satisfies a predetermined distribution condition.